

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

CHANDRA MCPHERSON, on behalf of)	
herself and all others similarly situated,)	
)	No. 1:13-cv-9188
Plaintiff,)	
)	
v.)	JURY TRIAL DEMANDED
)	
TARGET CORPORATION, a)	
Minnesota corporation,)	
)	
Defendant.)	

CLASS ACTION COMPLAINT

Plaintiff Chandra McPherson (“Plaintiff”) brings this Class Action Complaint against Defendant Target Corporation (“Defendant” or “Target”), individually and on behalf of all others similarly situated, and complains and alleges upon personal knowledge as to herself and her own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Target for its failure to secure and safeguard its customers’ personal financial data, including credit and debit card information.

2. On December 19, 2012, Target disclosed a data breach involving an extensive nationwide theft of customers’ credit-card and debit-card data—one of the largest data breaches ever, with 40 million compromised customer accounts. The breach occurred when hackers (referred to herein as “skimmers”) infiltrated Target’s flawed payment security system and accessed Target customers’ personal financial data by way of the Target PIN pad swipe terminals at the retail point of sale (the “Security Breach”).

3. Target's security failures enabled the skimmers to steal financial data from within Target's stores and, on information and belief, subsequently make unauthorized purchases on customers' credit cards and otherwise put Class members' financial information at serious and ongoing risk. The skimmers continue to use the information they obtained as a result of Target's inadequate security to exploit and injure Class members across the United States.

4. The Security Breach was caused and enabled by Target's knowing violation of its contractual obligations to abide by best practices and industry standards concerning the security of PIN pad terminals. Target grossly failed to comply with security standards and allowed their customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

5. Accordingly, Plaintiff, on behalf of herself and other members of the Class, asserts claims for breach of implied contract and violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*, and seeks injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

6. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiff's claims and the claims of the other members of the Class exceed \$5,000,000 exclusive of interest and costs, and there are numerous class members who are citizens of States other than Target's State of citizenship.

7. This Court has personal jurisdiction over Target because Target is registered with the Illinois Secretary of State to conduct business in the State of Illinois, and does conduct

substantial business in the State of Illinois, such that Target has significant continuous and pervasive contacts with the State of Illinois. Target also maintains numerous stores and employees in the State of Illinois, including multiple stores compromised in the Security Breach.

8. Venue is proper in this District pursuant to 28 U.S.C. §§ 1301(a)(2), 1391(b)(2), and 1391(c)(2) as: a substantial part of the events and/or omissions giving rise to the claims emanated from activities within this District, and Target conducts substantial business in this District.

III. PARTIES

Plaintiff McPherson

9. Chandra McPherson is a citizen of Illinois and resides in Cook County, Illinois. Plaintiff shopped at a Target retail location in California. Plaintiff swiped her debit card through one of the store's PIN pad terminals and, as a result, entered into an implied contract with Target for the adequate protection of her debit card information, and had her sensitive financial information exposed as a result of Target's inadequate security.

10. Plaintiff's bank, Chase, has since informed Plaintiff that she is considered "at risk" as a result of the data breach, and, as a result, Chase restricted her daily cash withdrawal and daily purchase limits.

Defendant Target

11. Target Corporation is a Minnesota corporation with its principal place of business in Minneapolis, Minnesota. Target is the second-largest discount retailer in the United States and is ranked 36th on the Fortune 500 list of top United States companies by revenue.

IV. FACTUAL BACKGROUND

PIN Pad “Skimming”

12. Like many other retailers, Target uses PIN pad terminals to process its customers’ in-store debit and credit card payments.

13. A PIN pad is an electronic device used in a debit or credit card-based transaction. To make a debit or credit card purchase through a PIN pad, a cardholder swipes their credit or debit card through the PIN pad and then inputs their PIN. A properly operating PIN pad will then encrypt the cardholder’s PIN, temporarily store the encrypted PIN – along with other card and transaction information – and then transmit that information to a transaction manager or bank for verification to complete the transaction.

14. “Skimming” is a form of electronic system hacking that enables the unauthorized capture of debit and/or credit card magnetic strip data by unauthorized persons. These unauthorized persons are often referred to as “skimmers.”

Target’s Contractual Obligation to Protect Customer Information

15. Target accepts customer payments for purchases through credit and debit cards issued by members of the payment card industry (“PCI”) such as Visa USA (“Visa”), MasterCard, Discover, and American Express. Some card issuers, like Visa, contractually obligate merchants, like Target, to comply with various PIN pad security standards that protect customer financial information as a condition of being permitted to process transactions through the card issuer.

16. At all times relevant to this action, Target was authorized by Visa to accept Visa credit and debit cards for the payment of personal goods.

17. Visa is a privately-held for profit association that supplies and supports Visa credit and debit cards issued by financial institutions to their customers by providing an authorization service for Visa card transactions and a clearing and settlement service to transfer payment information between parties involved in credit and debit card transactions. Visa is a member of the PCI.

18. In 2005, Visa issued a global mandate (“Visa’s Global Mandate”), requiring that by July 1, 2010, each of its merchants authorized to accept payment through Visa debit and credit cards discontinue the use of PIN pad terminals that do not meet the Triple Data Encryption Standard (“TDES”). TDES compliant devices provide greater security than earlier generation devices. With respect to the enhanced security protections of Visa’s Global Mandate, David Ottenheimer, a payments security expert who works with the technology consultancy K3DES LLC recently noted the importance of upgrading to tamper resistant equipment, stating: “If you have a device that’s five years old, it probably doesn’t have the protections that it would need” to ward off fraud.

19. Target is contractually obligated to fully comply with Visa’s Global Mandate as a condition of being permitted to process transactions through the Visa network.

20. Visa also created operating regulations for merchants who elect to accept its cards, which include a list of thirty-two requirements that those merchants must implement to protect the security of cardholder information (the “PCI PIN Security Requirements”).¹

21. The PCI PIN Security Requirements, include the following:

- Requirement 1. “All cardholder-entered PINs are processed in equipment that conforms to the requirements for tamper-resistant security modules.”

¹ See Payment Card Industry PIN Security Requirements, version 2.0 January 2008, located at http://usa.visa.com/download/merchants/pci_pin_security_requirements_2008.pdf (last visited Dec. 19, 2013).

- Requirement 29. “PIN-processing equipment is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.” Visa further notes that, in compliance with international and industry standards, merchants must implement procedures that “*include ensuring that a counterfeit device possessing all the correct operational characteristics plus fraudulent capabilities has not been substituted for a legitimate device.*”
- Requirement 32. “Documented procedures exist and are demonstrably in use to ensure the security and integrity of PIN-processing equipment placed into service, initialized, deployed, used, and decommissioned.”

22. Target is contractually obligated to fully comply with the PCI PIN Security Requirements as a condition of being permitted to process transactions through the Visa network.

23. Visa warns that “merchant non-compliance (with the PCI PIN Security Requirements) could potentially subject the Visa payment system to an extremely high level of risk.”² Similarly, a merchant’s non-compliance with the PCI PIN Security Requirements subjects its customers to an extremely high level of risk.

24. In 2006, Visa, MasterCard, and other PCI members established the Security Standards Council (“PCI SSC”). PCI SSC is an open global forum responsible for the development, management, education, and awareness of PCI Data Security Standard and related standards for increased security of PIN pad terminals.

25. In addition to developing security standards applicable to payment card processing generally, PCI SSC developed even more stringent standards for PIN pad terminals (referred to by the PCI SSC as “PCI PIN Entry Devices” or “PCI PEDs”) in order, among other things, to make PIN pad terminals more tamper-resistant.³

² See PIN Security, Tools and Best Practices for Merchants, at 3, located at <http://usa.visa.com/download/merchants/pin-security-080507-final.pdf> (last visited Dec. 19, 2013).

³ See Payment Card Industry PIN Security Requirements, version 2.0, January 2008 at 77.

26. Since December 31, 2007, PCI members require that merchants who accept their credit or debit cards do not put into service PIN pad terminals that fail to meet the PCI PED standard.⁴

27. Target is contractually obligated – as a condition of being permitted to process transactions through PCI companies – to fully comply with the PCI PED requirements and other requirements concerning the security of customer financial information.

Security Breaches Lead to Identity Theft

28. The United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”) that identity thieves use personal identifying data to open financial accounts, receive government benefits and incur charges and credit in a person’s name.⁵ As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim’s credit rating. In addition, the GAO Report states that victims of identity theft will face “substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name.”

29. According to the Federal Trade Commission (“FTC”), identity theft wreaks havoc on consumer’s finances, credit history and reputation and can take time, money and patience to resolve.⁶ Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.⁷

⁴ *Id.*

⁵ See <http://www.gao.gov/new.items/d07737.pdf>.

⁶ See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), <http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf> (last visited Dec. 19, 2013).

⁷ The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 CFR § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security

30. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

31. Personal identifying information (“PII”) – like the Target’s customer names combined with their credit or debit card information that were stolen in the Security Breach at issue in this action– is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for a number of years.⁸ As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, and other PII directly on various Internet websites making the information publicly available.

The Monetary Value of Privacy Protections

32. At a Federal Trade Commission (“FTC”) public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer’s personal information as follows:

The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it’s

number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

⁸ Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation’s Norton brand has created a software application that values a person’s identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. See also T. Soma, ET AL, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009).

something on the order of the life blood, the free flow of information.⁹

33. Though Commissioner's Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a \$26 billion per year online advertising industry in the United States.¹⁰

34. The FTC has also recognized that consumer data is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.¹¹

35. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent, consumers will make a profit from the surrender of their PII.¹² This business has created a new market for the sale and purchase of this valuable data.¹³

⁹ *The Information Marketplace: Merging and Exchanging Consumer Data*, <http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm> (last visited Dec. 20, 2013).

¹⁰ *See Web's Hot New Commodity: Privacy*, <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html> (last visited Dec. 20, 2013).

¹¹ *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited Dec. 20, 2013).

¹² *You Want My Personal Data? Reward Me for It*, <http://www.nytimes.com/2010/07/18/business/18unboxed.html> (last visited Dec. 20, 2013).

¹³ *See Web's Hot New Commodity: Privacy*, <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html> (last visited Dec. 20, 2013).

36. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that “when [retailers’] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”¹⁴

37. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use – two concerns at issue here – they valued the restriction of improper access to their data at between \$11.33 and \$16.58 per website, and prohibiting secondary use to between \$7.98 and \$11.68 per website.¹⁵

38. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers’ PII has thus deprived that consumer of the full monetary value of the consumer’s transaction with the company.

The Target Data Breach

39. On December 19, 2013, Target reported the Security Breach, and stated the Breach occurred from November 27 through December 15 in stores nationwide—roughly 40,000 card devices.¹⁶ The affected data includes customer names, credit and debit-card numbers, expiration dates, and three-digit security codes embedded in the magnetic stripe.¹⁷

¹⁴ Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, available at <http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (emphasis added) (last visited Dec. 20, 2013); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

¹⁵ *Id.*

¹⁶ Rubin Sidel, et al., *Target Hit By Breach of Credit Cards*, Wall Street Journal, December 19, 2013, at B1.

¹⁷ Sara Germane, et al., *Target Faces Breach Backlash*, Wall Street Journal, December 20, 2013, at B1.

40. Many Class members have already complained of unauthorized, fraudulent charges in the compromised accounts.¹⁸

41. Moreover, the credit and debit cards stolen in the Security Breach “have been flooding underground markets in recent weeks, selling in batches of 1 million cards and going for anywhere from \$20 to more than \$100 per card.”¹⁹

42. Class members – including the Plaintiff – have also had their daily purchase and cash withdrawal limits significantly lowered and restricted as a direct result of the Security Breach, which has impeded the ability of Class Members to purchase items at the height of the Christmas shopping season.

43. On information and belief, at the time of the Security Breach, Target was not in compliance with Visa’s Global Mandate that requires the use of tamper-resistant PIN pads in all of its stores. Target also failed to comply with the PCI PIN Security Requirements.

44. Target’s failure to comply with Visa’s Global Mandate and the PCI PIN Security Requirements provided Target with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of Target’s own customers – including Class members here – who have been subject to the Security Breach or otherwise have had their financial information placed at serious and ongoing risk.

45. Target allowed widespread and systematic theft of its customers’ financial information. Target’s actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers’ financial information. Despite being contractually obligated to do so, Target failed to employ appropriate technical, administrative, or physical procedures to protect its customers’ financial information from unauthorized capture,

¹⁸ Tiffany Hsu, et al., *Data Thieves Are Seeing Green On Black Market*, Chicago Tribune, December 21, 2013, at 5.

¹⁹ *Id.*

dissemination, or misuse, thereby making its customers easy targets for theft and misuse of their financial information, including in the manner undertaken by the skimmers here.

Damages Sustained By Plaintiff and the Class

46. A portion of the services purchased from Target by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PII, including their credit card information. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the products purchased from Target.

47. Plaintiff and the Class have suffered additional injury in fact and actual damages including monetary losses arising from unauthorized bank account withdrawals and/or related bank fees charged to their accounts.

48. Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Target's wrongful conduct, particularly given the incidents of actual misappropriation from Class members' financial accounts, as detailed above.

49. Plaintiff and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend to monitor their financial and bank accounts as a result of the Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

50. Plaintiff and the Class suffered additional damages to the extent Class members' banks have reduced daily transaction withdrawal limits to protect the banks' own risk.

V. CLASS ACTION ALLEGATIONS

51. Plaintiff brings Counts I and II, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

All persons residing in the United States who made an in-store purchase at a Target store using a debit or credit card that was swiped through a PIN pad at any time from November 27, 2013 through December 15, 2013 (the “National Class”).

Excluded from the National Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

52. Plaintiff brings Count II, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

All persons residing in one of the Consumer Fraud States²⁰ who made an in-store purchase at a Target store using a debit or credit card that was swiped through a PIN pad at any time from November 27, 2013 through December 15, 2013 (the “Consumer Fraud Multistate Class”).

²⁰ The States that have similar consumer fraud laws based on the facts of this case are: Arkansas (Ark. Code § 4-88-101, *et seq.*); California (Cal. Bus. & Prof. Code §17200, *et seq.* and Cal. Civil Code § 1750, *et seq.*); Colorado (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut (Conn. Gen. Stat. § 42-110, *et seq.*); Delaware (Del. Code tit. 6, § 2511, *et seq.*); District of Columbia (D.C. Code § 28-3901, *et seq.*); Florida (Fla. Stat. § 501.201, *et seq.*); Hawaii (Haw. Rev. Stat. § 480-1, *et seq.*); Idaho (Idaho Code § 48-601, *et seq.*); Illinois (815 ICLS § 505/1, *et seq.*); Maine (Me. Rev. Stat. tit. 5 § 205-A, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws § 445.901, *et seq.*); Minnesota (Minn. Stat. § 325F.67, *et seq.*); Missouri (Mo. Rev. Stat. § 407.010, *et seq.*); Montana (Mo. Code. § 30-14-101, *et seq.*); Nebraska (Neb. Rev. Stat. § 59-1601, *et seq.*); Nevada (Nev. Rev. Stat. § 598.0915, *et seq.*); New Hampshire (N.H. Rev. Stat. § 358-A:1, *et seq.*); New Jersey (N.J. Stat. § 56:8-1, *et seq.*); New Mexico (N.M. Stat. § 57-12-1, *et seq.*); New York (N.Y. Gen. Bus. Law § 349, *et seq.*); North Dakota (N.D. Cent. Code § 51-15-01, *et seq.*); Oklahoma (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon (Or. Rev. Stat. § 646.605, *et seq.*); Rhode Island (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Dakota (S.D. Code Laws § 37-24-1, *et seq.*); Virginia (VA Code § 59.1-196, *et seq.*); Vermont (Vt. Stat. tit. 9, § 2451, *et seq.*); Washington (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia (W. Va. Code § 46A-6-101, *et seq.*); and Wisconsin (Wis. Stat. § 100.18, *et seq.*).

Excluded from the Consumer Fraud Multistate Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

53. In the alternative, Plaintiff brings Count II, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

All persons residing in the State of Illinois who made an in-store purchase at a Target store using a debit or credit card that was swiped through a PIN pad at any time from November 27, 2013 through December 15, 2013 (the “Illinois State Class”).

Excluded from the Illinois State Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

54. The National Class, Consumer Fraud Multistate Class, and Illinois State Class are collectively referred to as the “Class,” unless specifically indicated otherwise.

55. Certification of Plaintiff’s claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

56. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, Class members number in the thousands. The precise number of Class members and their addresses are presently unknown to Plaintiff, but may be ascertained from Target’s books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

57. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

- a. Whether Target failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive financial information;
- b. Whether Target properly implemented its purported security measures to protect customer financial information from unauthorized capture, dissemination, and misuse;
- c. Whether Target's conduct violates the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*;
- d. Whether Target's conduct constitutes breach of an implied contract;
- e. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

58. Target engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

59. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Target's uniform misconduct described above and were thus

all subject to the Security Breach alleged herein. Further, there are no defenses available to Target that are unique to Plaintiff.

60. Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).

Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other Class members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation; and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and her counsel.

61. Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).

Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Target. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

62. Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).

Target has acted or refused to act on grounds generally applicable to Plaintiff and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

63. Superiority – Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy,

and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Target, so it would be impracticable for Class members to individually seek redress for Target's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED

COUNT I

Breach of Implied Contract (On Behalf of the National Class)

64. Plaintiff incorporate paragraphs 1-63 as if fully set forth herein.

65. Target's customers who intended to make in-store purchases with debit or credit cards were required to provide their card's magnetic strip data and PINs (for debit cards) for payment verification.

66. In providing such financial data, Plaintiff and the other members of the Class entered into an implied contract with Target whereby Target became obligated to reasonably safeguard Plaintiff's and the other Class members' sensitive, non-public, information.

67. Target breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their financial data.

68. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to loss of their financial information, loss of money and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

COUNT II

**Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
(and Substantially Similar Laws of the Consumer Fraud States²¹)
(on Behalf of the Consumer Fraud Multistate Class)**

69. Plaintiff incorporates paragraphs 1-63 as if fully set forth herein.

70. Plaintiff and the other members of the Class were deceived by Target's failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while shopping at Target.

71. Target intended for Plaintiff and the other members of the Class to rely on Target to protect the information furnished to it in connection with their debit and credit card transactions, in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

72. Target instead handled Plaintiff and the other Class members' personal information in such manner that it was compromised.

73. Target either willfully ignored its contractual obligations to Visa and other PCI members and failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

74. It was foreseeable that Target's willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

²¹ The Consumer Fraud States were defined at *supra* note 20.

75. Target benefited from mishandling its customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Target saved on the cost of those security measures.

76. Target's fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class members' reliance on Target's deception that their financial information was secure and protected when using debit and credit cards to shop at Target.²²

77. Target violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the other members' private financial information.

78. Target's acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

79. Target's conduct constitutes unfair acts or practices as defined in that statute because Target caused substantial injury to Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

80. Plaintiff and the other members have suffered injury in fact and actual damages including lost money and property as a result of Target's violations of 815 ILCS 505/2.

81. Plaintiff's and the other Class members' injuries were proximately caused by Target's fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

²² The consumer protection statutes or interpretive law of the Consumer Fraud States have also either: (a) expressly prohibited omissions of material fact, without regard for reliance on the deception, or (b) have not addressed those issues.

82. By this conduct, Target violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of Illinois, or conflict with each other for purposes of this action.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this complaint so triable.

VIII. REQUEST FOR RELIEF

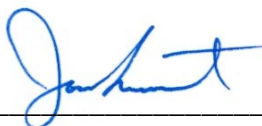
WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Target, as follows:

- A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative and appointing the undersigned counsel as Class Counsel for the Class;
- B. Ordering Target to pay actual damages to Plaintiff and the other members of the Class;
- C. Ordering Target to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;
- D. Ordering Target to pay statutory damages, as provided by the Illinois Consumer Fraud and Deceptive Business Practices Act and other applicable State Consumer Fraud Acts, to Plaintiff and the other members of the Class;
- E. Ordering Target to disseminate individualized notice of the Security Breach to all Class members and to post notice of the Security Breach in all of its affected stores;
- F. Ordering Target to pay attorneys' fees and litigation costs to Plaintiff and the other members of the Class;
- G. Ordering Target to pay both pre- and post-judgment interest on any amounts awarded; and
- H. Ordering such other and further relief as may be just and proper.

Dated: December 24, 2013

Respectfully submitted,

CHANDRA MCPHERSON, individually and
on behalf of all others similarly situated

By: _____

Attorneys for Plaintiff
And the Proposed Putative Classes

Joseph J. Siprut
jsiprut@siprut.com
Gregg M. Barbakoff
gbarbakoff@siprut.com
Gregory W. Jones
gjones@siprut.com
SIPRUT PC
17 North State Street
Suite 1600
Chicago, Illinois 60602
312.236.0000
Fax: 312.470.6588

4845-5671-0167, v. 1